

Serial No. 09/852,262
HP 30003063-2 US
LHGB 1509-172
Page 2

IN THE CLAIMS:

Please amend claims 1, 3, 6, 7, 14, 16, 18, and 22-24 as follows:

1. (Currently amended) A distributed storage system for storing at least one credential, provided by an issuing authority relating to an identity, the system comprising:

at least one unique identity having a local store, the store of the at least one identity securely storing one or more credentials relating to the owner of the identity; and

a security certificate provided at each identity for ensuring the authenticity of the one or more credentials, the ~~security~~ security certificate providing a secure reference to the issuer of the one or more credentials that can be used in verifying the origin of each credential, the store being accessible by parties other than the owner and being arranged so the parties other than the owner are able to read the credentials and security certificates of the owner.

2. (Previously presented) A system according to Claim 1, wherein the at least one identity comprises a hierarchical structure.

3. (Currently amended) A system according to ~~Claim2~~ Claim 2, wherein the at least one identity comprises at least one

Serial No. 09/852,262
HP 30003063-2 US
LHGB 1509-172
Page 3

role, the role being a subset of the identity having its own credentials within the identity.

4. (Previously presented) A system according to Claim 1, further comprising a host site, the host site having a plurality of identities and associated stores.

5. (Previously presented) A system according to Claim 4, wherein the host site comprises a management module for managing data access to and from the each of the identities and their associated stores.

6. (Currently amended) A system according to Claim 4, wherein the host site comprises a ~~trust~~ trusted financial institution's website.

7. (Currently amended) A system according to Claim 1, wherein the identity or host site comprises a website.

8. (Previously presented) A system according to Claim 7, wherein the identity further comprises a homepage for providing general information regarding the identity.

9. (Previously presented) A system according to Claim 1, wherein the local store of the identity comprises a portable mobile device which is connectable to a telecommunications network.

Serial No. 09/852,262
HP 30003063-2 US
LHGB 1509-172
Page 4

10. (Previously presented) A system according to Claim 1, wherein the identity is arranged to store a private key of the identity for encryption of the identity.

11. (Previously presented) A system according to Claim 10, wherein the identity is arranged to store a public key of the identity for decryption of the identity.

12. (Previously presented) A system according to Claim 11, wherein the public key of the identity is embedded within each credential of the identity.

13. (Previously presented) A system according to Claim 1, wherein the identity is arranged to store a public key of the authority which has issued the one or more credentials to the identity.

14. (Previously presented) A system according to Claim 13, wherein the public keys for each of the at least one role and the identity are stored in the appropriate store or identity.

15. (Previously presented) A system according to Claim 1, wherein at least some of the credentials are arranged to be encrypted.

16. (Currently amended) A system according to Claim 1, wherein the one or more credentials each ~~refer~~ refers to the corresponding security certificate.

Serial No. 09/852,262
HP 30003063-2 US
LHGB 1509-172
Page 5

16. (Currently amended) A system according to Claim 1, wherein the one or more credentials each ~~refer~~ refers to the corresponding security certificate.

17. (Previously presented) A system according to Claim 1, wherein the security certificate comprises information describing the issuer, the identity to whom the certificate has been issued, a validity period and a list of credentials to which the certificate relates.

18. (Currently amended) A system according to Claim 1, wherein the certificate is digitally signed using a private key and the certificate contains ~~[[the]]~~ a public key for reading the digital signature.

19. (Previously presented) A system according to Claim 1, wherein the identity further comprises a generator module for generating a certificate regarding the identity for use in proxying credentials to the store of a different identity.

20. (Previously presented) A system according to Claim 1, wherein the identity further comprises a mailbox for receiving messages from other identities.

21. (Previously presented) A system according to Claim 20, wherein the identity further comprises an authorization function

Serial No. 09/852,262
HP 30003063-2 US
LHGB 1509-172
Page 6

module arranged to check that a request for access to the mailbox has originated from an authorized identity.

22. (Currently amended) A method of storing credentials relating to identities provided by an issuing authority in a distributed manner, the method comprising:

securely storing one or more credentials relating to the owner of an identity in a local store of the identity; [[and]]

providing a security certificate at the identity for ensuring the authenticity of the one or more credentials, the security certificate providing a secure reference to the issuer of the one or more credentials that can be used in verifying origin of each credential; and

accessing the store by parties other than the owner who read the credentials and security certificates of the owner.

23. (Currently amended) An identity of an entity for making available credentials belonging to the entity to other entities, each entity comprising:

a local store arranged to securely hold one or more credentials relating to the entity; and

a certificate processing module for reading and verifying received security certificates and creating security certificates for transmission, the security certificates providing a secure reference to the issuer of the one or more

Serial No. 09/852,262
HP 30003063-2 US
LHGB 1509-172
Page 7

credentials that can be used in verifying the origin of each credential, the store being accessible by parties other than the owner and being arranged so the parties other than the owner are able to read the credentials and security certificates of the owner.

24. (Currently amended) A distributed storage system for storing a plurality of credentials, the system comprising:

a plurality of identities for making available credentials belonging to an entity to other entities, each entity comprising a local store arranged to securely hold one or more credentials relating to the entity; and

a certificate processing module for reading and verifying received security certificates and creating security certificates for transmission, the security certificates providing a secure reference to the issuer of the one or more credentials that can be used in verifying the origin of each credential, the store being accessible by parties other than said entity and being arranged so entities other than said entity are able to read the credentials and security certificates of said entity.